INSTITUTE FOR DEFENSE ANALYSES

Department of Defense Use of Commercial Cloud Computing Capabilities and Services

Laura A. Odell, *Project Leader*

Ryan R. Wagner
Tristan J. Weir

November 2015

IDA Paper
P-5287
Log: H 15-000865
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-3975, "Measuring DoD Use of Commercial Cloud Computing Capabilities and Services," for Deputy CIO for Information Environment, DoD CIO. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
Ronald G. Bechtold, Dale Visser

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-5287

Department of Defense Use of Commercial Cloud Computing Capabilities and Services

Laura A. Odell, *Project Leader*

Ryan R. Wagner
Tristan J. Weir

Executive Summary

U.S. House of Representatives Report 113-446, National Defense Authorization Act for Fiscal Year (FY) 2015, directed the Secretary of Defense to "conduct an independent assessment of the Department's policies and guidance for cloud computing capabilities." In addition, U.S. Senate Report 113-176, National Defense Authorization Act for FY 2015 directed the Department of Defense (DoD) Chief Information Officer (CIO) to "sponsor an independent study to develop metrics to assess DoD's progress in evaluating and adopting commercial cloud capabilities," as well as compare "milCloud … to the leading commercial cloud technology."

In April 2015, the DoD CIO asked the Institute for Defense Analyses (IDA) to provide an independent assessment of DoD's adoption of commercial cloud technologies and services. This report directly responds to both the House and Senate's requests, but it also identifies new opportunities and challenges that DoD is encountering as it moves its data and applications into a cloud environment. IDA performed this research between April and August 2015.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of computing resources. It helps organizations rapidly scale up capabilities, achieve cost-effective economies of scale, and maintain resiliency. At the same time, cloud computing introduces transition costs and security concerns.

In 2015, DoD is taking action to offer a wider selection of commercially owned and operated cloud services to DoD mission owners. Currently, mission owners desiring to move to the cloud can choose from 32 authorized cloud service offerings in a variety of configurations with varying levels of security. Some offerings provide complete cloud-enabled software packages while others offer infrastructure or platforms on which to host legacy applications or build new ones.

Much of DoD's data is sensitive, so the cloud environment must maintain confidentiality and integrity of that data. DoD has instituted a process to evaluate and issue Provisional Authorizations for cloud service offerings, based on the security controls that the provider implements and the sensitivity level of the data that it intends to host. The DoD Cloud Computing Security Requirements Guide specifies the key elements that a commercial cloud provider must meet to qualify for each data sensitivity level. Of the 32 authorized cloud service offerings, DoD authorizes two to host some of the most sensitive data (e.g., Personally Identifiable Information, For Official Use Only);

the rest are authorized to host non-sensitive, publicly releasable information. DoD mission owners can also host applications on milCloud, the private cloud offering built by the Defense Information Systems Agency (DISA). MilCloud offers some of the features of commercial providers with enhanced security that comes from DoD operation and monitoring.

Cloud computing is a relatively new field, and there are no widely accepted metrics for measuring cloud adoption rates or benchmarks for organizations transitioning to the cloud. IDA identified and developed several broad categories of metrics that can measure DoD's cloud adoption and the value provided by commercial cloud offerings. They include:

- Statistics for Cloud Service Offering Adoption – provides an objective measure of the availability and types of cloud service offerings,
- Value through Cost Savings/Cost Avoidance – provides a measure of the financial value of transitioning data and applications to a commercial cloud environment,
- Value through Usability – provides a measure of the ease with which DoD mission owners can acquire and use commercial cloud services,
- Value through Automation – provides a measure of how the cloud environment is reducing IT labor requirements for the setup and maintenance of cloud instantiations,
- Value through Availability – provides a measure of how much uptime the cloud environment is achieving,
- Value through Security and Compliance – provides a measure of the confidentiality, integrity, and availability of data in the cloud.

The timing of DoD's move toward the commercial cloud is reasonable given the risk and assurance requirements of many of its missions. DoD has positioned itself as a fast follower, not committing to a specific technology or new business model until the market has matured. DoD mission owners have significant latitude when choosing which of their data and applications belong in the cloud, but the DoD Chief Information Officer should offer better guidance about the risks of cloud computing and what mission owners should consider as they mitigate or avoid those risks. In addition, mission owners need to weigh the additional costs and risks of transitioning legacy applications into the cloud versus building new cloud-native applications.

DoD's approach to commercial cloud security relies on the cloud provider implementing specified security controls. However, DoD has recently contemplated providing a common set of security services (at scale) that all providers can leverage to achieve better across-the-board security. One remaining concern for several commercial

providers is the requirement of physical isolation of cloud servers for the most sensitive unclassified data. Cloud economies of scale rely on a shared resources model across multiple organizations, and the current requirements may be in conflict with that premise. We recommend that DoD consider allowing its Defense Industrial Base partners to participate in high-sensitivity community cloud infrastructure, thereby increasing the efficiency and utility of those systems.

Contents

Figures and Tables

1. Background

A. Congressional Request

U.S. House of Representatives Report 113-446, National Defense Authorization Act for Fiscal Year (FY) 2015, directed the Secretary of Defense to "conduct an independent assessment of the Department's policies and guidance for cloud computing capabilities." The assessment would include an analysis of the Department's:

- Implementation of industry and government best practices for commercial cloud computing,
- Commercial cloud brokerage procedures,
- Cloud security protocols,
- Integration of cloud capabilities into the Joint Information Environment (JIE),
- Metrics by which commercial cloud pilots are evaluated.

In addition, U.S. Senate Report 113-176, National Defense Authorization Act for FY 2015 directed the Department of Defense (DoD) Chief Information Officer (CIO) to "sponsor an independent study to develop metrics to assess DoD's progress in evaluating and adopting commercial cloud capabilities.…The study also should assess and compare the features, performance, costs, and functionality of the "milCloud" (military cloud) developed by the Defense Information Systems Agency using government contractors to the leading commercial cloud technology."

In April 2015, the DoD CIO asked the Institute for Defense Analyses (IDA) to provide an independent assessment of DoD's adoption of commercial cloud technologies and services. This report directly responds to both the House and Senate's requests, but it also identifies new opportunities and challenges that DoD is encountering as it moves its data and applications into a cloud environment. IDA performed this research between April and August 2015.

B. Overview of Cloud Computing

Cloud computing, as defined by the National Institute for Standards and Technology (NIST), is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2011) This definition outlines five essential characteristics (on-demand self-service, broad

network access, resource pooling, rapid elasticity, and measured service), three service models (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), and four deployment models (Public, Private, Community, and Hybrid) that further describe cloud computing.

1. Characteristics of Cloud Computing

a. On-demand Self-service

With on-demand self-service, a consumer can unilaterally provision computing capabilities automatically without requiring human interaction with a cloud service provider. (NIST, 2011) Consumers acquire capabilities such as server time and network space through a web-based control panel or Application Programming Interface (API). In this automated setting, the cloud service provider (CSP) cannot assume specialized technical knowledge on the consumer's part. Therefore, the provider should design an understandable user interface with settings that make sense to a non-technical user. (Sinnema, On Demand Self-Service, n.d.) The self-service capability allows the information technology (IT) labor force to focus less on collecting customer requirements and more on planning and designing new capabilities. A reduction in customization drastically reduces costs associated with offering IT services.

b. Broad Network Access

Broad network access refers to cloud computing resources being accessible over the network through any standard heterogeneous client platform such as mobile phones, tablets, laptops and desktop computers. (NIST, 2011) Consumers can use these devices to access the cloud from any location via a simple web-based access point. (The Open Group, 2013) A popular example of this characteristic is a consumer's ability to access web-based email, such as Gmail and Yahoo, from any device. Administrators can also access and provision cloud resources from outside a specialized corporate network, allowing rapid satisfaction of service requests. This mobility is especially advantageous to consumers who frequently need to access information while mobile or from a telework location.

c. Resource Pooling

With resource pooling, the cloud service provider's pools its computing resources to serve a large number of simultaneous consumers. Different physical and virtual resources, such as storage, processing, memory, and network bandwidth, are dynamically assigned according to consumer demand. (NIST, 2011) The virtual resources of cloud service offerings (CSO) tenants are logically isolated from each other, but draw from the same physical infrastructure because they are co-located in the same facilities. Pooling

resources builds economies of scale, which in turn lowers costs for consumers. It also removes inhibitors from the environment and increases efficiency by reducing crowding. (Benson, 2013) However, resource pooling may introduce security concerns, because the consumer typically has no control over the location of the provided resource or knowledge of other organizations that are sharing the resource. For data security, performance, and compliance with regulations, consumers may be able to specify their computing resource location generally, such as by country, state, or data center. (The Open Group, 2013)

d. Rapid Elasticity

Elasticity is the capability for an enterprise to scale up and down their operations within a cloud environment. (He & L. Guo, 2011) Computing capabilities can be flexibly provisioned and released, in some cases automatically, to rapidly scale up and down in accordance with consumer demand. (NIST, 2011) Resource pooling helps providers achieve elasticity because different services running on the cloud can have different workload patterns (seasonal, batch, etc.), and these differences allow the provider to balance the workload. (Sinnema, Rapid Elasticity, n.d.) Furthermore, the available capabilities appear unlimited to the consumer and can be accessed in any quantity, at any time. (NIST, 2011) The ability to scale at will requires providers to dynamically provision new computing resources based on demand monitoring. (Sinnema, Rapid Elasticity, n.d.) In combination with the pay-per-use billing model, the elasticity of the cloud provides consumers with significant savings. A common example of this is a retail web site that is accustomed to a consistent number of customers except during specific times of the year. A sudden rise in product demand during the holiday shopping season will increase the traffic significantly. If the site is hosted on a traditional, dedicated server, the lack of resources could cause the site to become unreachable. However, if hosted in the cloud, the resources could be rapidly scaled up to meet the rise in demand, either by moving to larger server instances or by designing the site to be horizontally scalable across additional small server instances.

e. Measured Services

Cloud service providers automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service. Measuring resource usage can provide transparency for both the provider and the consumer. (NIST, 2011) This is especially important for the pay-per-use billing model because consumers need sufficient measurements to make purchasing and operational decisions. (The Open Group, 2013) Every aspect, such as compute performance, memory utilization, and network bandwidth, is measured to deliver precisely configured services to the consumer. (Benson, The Cloud Defined: Measured Service, 2013) For the provider, measurability

goes hand in hand with rapid elasticity, allowing providers to dynamically provision new computing resources to meet rapidly changing consumer needs.

2. Cloud Service Models

NIST defines three main models for cloud computing: IaaS, PaaS, and SaaS. These models help differentiate the implementation responsibilities that fall on the CSP from the responsibilities that fall on the customer. Each model serves a different need and provides a different level of capability to an organization. Figure 1-1 provides a discussion of each service model.

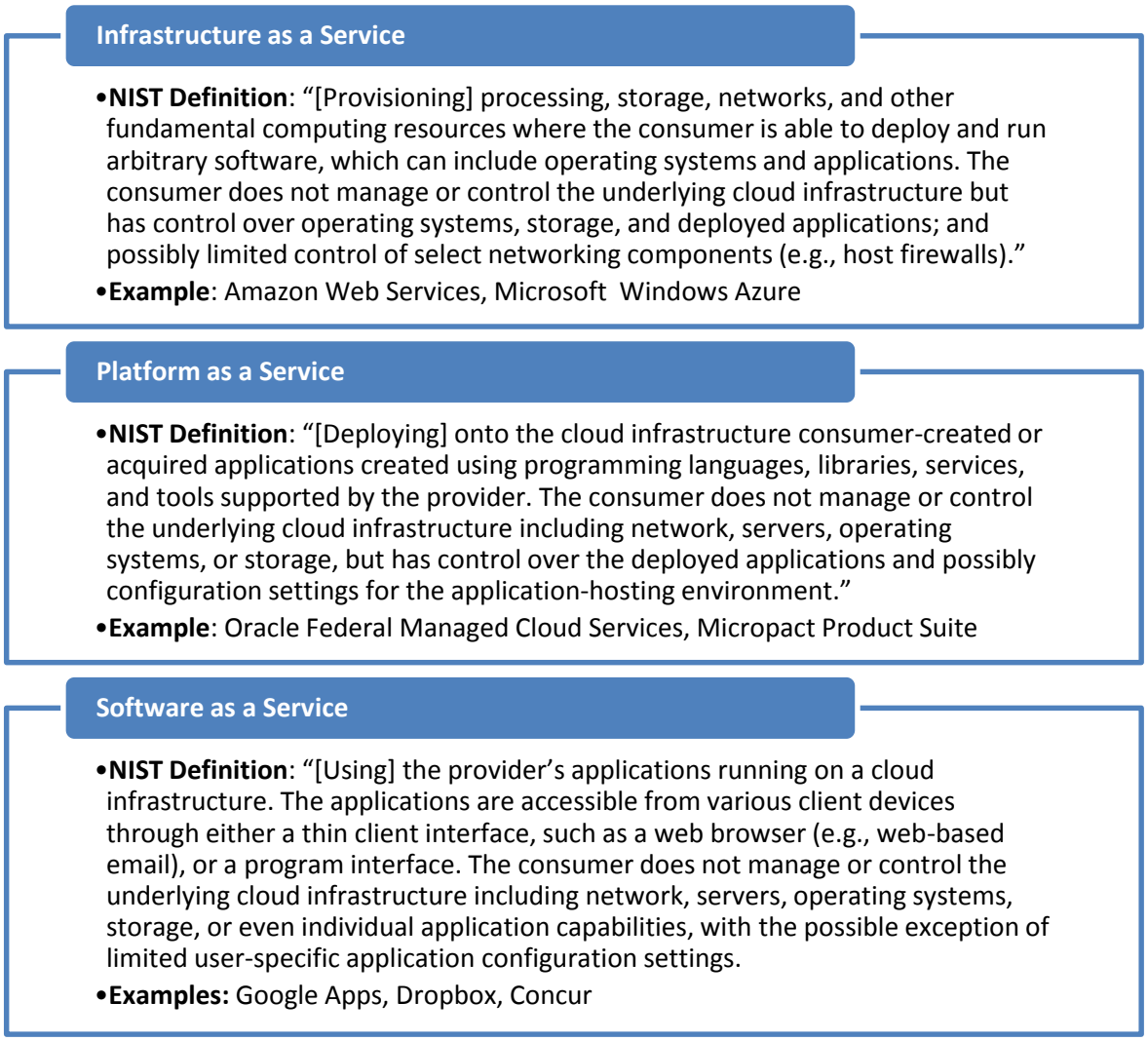

Figure 1-1. NIST Definitions of Cloud Service Models (Source: NIST, 2011)

Although not specified by NIST, the Anything as a Service (XaaS) nomenclature has created niche markets for delivery of specialized tools and capabilities (What is XaaS, 2010). For example, Disaster Recovery as a Service (DRaaS) allows organizations

to outsource their business continuity capabilities so that they do not need to invest in their own dedicated alternate sites. Monitoring as a Service (MaaS) allows organizations to leverage dedicated cybersecurity professionals who can watch for intrusions and malware across all of their client's networks. These specialized XaaS models are constantly emerging and therefore do not have standardized definitions as do IaaS, PaaS, and SaaS.

3. Public, Private, Community, and Hybrid Clouds

Cloud services come in different forms, depending on the customer's specific needs, including security, privacy, and budget. Public cloud infrastructures operate in a multi-tenant environment, with resources allocated for the general public. Public clouds tend to be large and provide economies of scale for their customers. However, public clouds heighten security and privacy concerns because an individual or organization can potentially access the same cloud instance. Conversely, private cloud infrastructures are operated only for an individual organization, although a commercial cloud provider may operate them. The organization can leverage the scalability and performance aspects of cloud computing, but the infrastructure is isolated from that of other organizations, improving security and privacy. Due to their specialized nature, private clouds can be just as costly as dedicated data centers. Community cloud infrastructures are private clouds provisioned for a specific community of interest with shared concerns, such as a government-only cloud. Finally, hybrid cloud infrastructures are combinations of any two or more of the other cloud infrastructures. Figure 1-2 provides more information on public and private cloud instantiations.

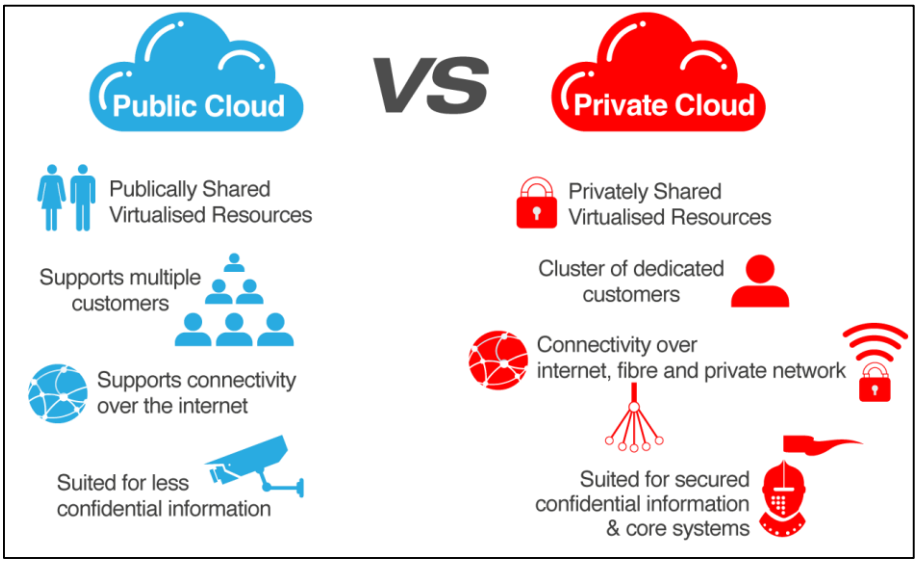

Figure 1-2. Public vs. Private Cloud (Source: Skali Group)

C. History of Cloud Computing

Although cloud computing is popularly viewed as a recent trend in IT, the concept originated in the 1950s with mainframe computing, where multiple users accessed the central mainframe through dumb terminals that provided shared access to a single source of storage and processing power. (Thoughts on Cloud, 2015) John McCarthy introduced the idea of computation as a public utility in 1961. (Mohamed, 2009) The idea was further matured in the 1960s by pioneers like J.C.R. Licklider, who was instrumental in the development of the Advanced Research Projects Agency Network (ARPANET). He envisioned a global computer network that allowed everyone to access programs and data anywhere. However, as processing moved from central mainframes to personal computers and dedicated servers in the 1980s and 1990s, the desire for centralized computer services waned.

It was not until the past decade that enhanced services and increased bandwidth allowed cloud computing to begin to transform commercial IT. (TechTarget, n.d.) (Mohamed, 2009) Companies became attracted to the benefits of cloud services such as reduced capital costs and reduced IT staffing. The present availability of high-capacity networks and low-cost computers, together with the adoptions of virtualization and service-oriented architecture, have led to present day cloud computing. (TechTarget, n.d.) Cloud services are also necessary to provide efficient storage and processing of the ever-increasing amount of data that industry collects. (Mohamed, 2009) As a result, industry has consistently increased its spending on cloud computing services to the extent that Forrester Research expects global public cloud purchases to rise from $72 billion in 2014 to $191 billion in 2020. (Bartles, Rymer, & Staten, 2014)

Major industry players such as Amazon, Google, Microsoft, and Salesforce, as well as small business and IT equipment manufacturers, have driven the evolution of modern cloud computing. Table 1-1 outlines some of the major developments in commercial cloud computing, and shows how the cloud has matured over time. It is important to note that many of the major changes have occurred within only the last few years.

Table 1-1. Major Historical Events in Cloud Computing

Year	Cloud Service Provider	Cloud Service Offering	Significance
1996	Microsoft	Hotmail	Pioneered SaaS e-mail.
1999	Salesforce.com		Pioneered the concept of delivering cloud-based business applications, which could be accessed by any customer with Internet access. Companies can purchase the service on an on-demand basis.
2002	Amazon	Amazon Web Services	Provides cloud-based computing services. Focuses on Amazon as a retailer and allows developers to build applications that makes Amazon features available to partners.
2005	Amazon	Mechanical Turk	Coordinates an on-demand, scalable, cloud-based human workforce to complete tasks that computers are unable to do.
2006	Amazon	Simple Storage Service (S3), Elastic Compute Cloud (EC2)	Launched a collection of cloud storage services. The real breakthrough was the pricing model for S3, which defined the model of pay-per-use, which has now become the standard for cloud pricing. EC2 made complete cloud computing infrastructure available, allowing users to run their own applications on the cloud. This disrupted the IT startup landscape by allowing small companies to rapidly build, scale, and demo new concepts.
2009	Google	Google Apps	The first widely adopted, low-cost, browser-based enterprise productivity application.
2013	Amazon	C2S Private Cloud	The Central Intelligence Agency awarded a $600-million, 10-year contract for an IC-wide cloud. Provides the IC with unprecedented access to various on-demand computing, analytic, storage, collaboration, and other services.

D. Benefits of Cloud Computing

In traditional computing models, an organization can grow its IT infrastructure by purchasing the necessary equipment or devices and integrating the new components into legacy systems. This is a costly and time-consuming activity, especially for smaller organizations that lack sufficient technical expertise and cannot afford rapid technology refresh cycles. Even after IT upgrades, the problems of underutilization of computing resources and managing complex IT networks persist. Cloud computing offers a solution with on-demand elasticity in IT services for any size enterprise. Elasticity helps smaller organizations avoid the large costs associated with rapidly scaling up their IT

infrastructure, freeing up capital for other critical needs. Cloud computing allows organizations to accommodate spikes in demand for their content by gaining the advantages of the economies of scale associated with pooling IT resources.

Cloud computing allows organizations to focus on their core missions and minimizes the distractions of building and managing IT solutions. For example, a Central Intelligence Agency (CIA) official reported that one of the major drivers for the CIA's move to a cloud environment was the desire to "get out of the business of racking and stacking servers." Transitioning to a cloud infrastructure could potentially result in higher productivity by allowing the reassignment of system administrators to other roles. Instead of routine IT tasks such as server management, that staff is able to perform high-level, business-focused activities like application development or optimization. Finally, simplified internal operations and business agility are additional advantages to using cloud computing, although the customer still needs to maintain contract oversight to ensure compliance with their requirements.

Cloud computing allows for rapid improvements to infrastructure, services, and technology that is not possible with traditional IT acquisitions. When commercial cloud providers add new services, the provider's customers can immediately use those services. When providers add new processing or storage capacity, consumers across the entire cloud infrastructure can see those speed improvements. The rapid evolution of technology and increased adoption of cloud platforms also leads to pricing that decreases over time. For example, between 2008 and 2014, Amazon announced 42 price reductions for its Amazon Web Services (AWS) offering. (Barr, 2014)

E. Concerns About Cloud Computing

Some of the primary concerns of a government organization considering using cloud computing are data security, latency, and unanticipated costs. Security and privacy of the data in the cloud is a critical issue for government consumers. Cloud promotes a shared environment in which multiple cloud tenants leverage the same infrastructure. Technical controls create virtual separation of data and applications for different tenants, but there are concerns that some users could access data across the virtual boundaries. In addition, regulatory requirements may prohibit comingling of government and commercial data on the same cloud platform. The distributed nature of cloud means that data could be physically located at data centers in high-risk countries.

Latency issues can be a concern because network traffic between users and remote cloud data centers can be slower than connections to local data centers. (Abdul, 2013) Cloud providers may have sufficient bandwidth to serve all of their customers, but bandwidth bottlenecks can still occur on the customer networks if those networks are not configured to support a more distributed architecture. Organizations seeking to utilize a cloud environment must ensure that their own network capacity is robust enough to

handle the traffic load, especially for cloud services other than simple web applications (Bright, 2013) As more applications are moved to the cloud and bandwidth demands increase, cloud customers must continue to upgrade and optimize their networks, often at increased cost.

Organizations transitioning to cloud computing frequently underestimate the cost or difficulty of integrating cloud with legacy systems. When legacy systems are ported into a cloud environment, they will generally not be able to take advantage of resource pooling, elasticity, and other desirable cloud features without significant software development or retrofitting. Organizations with virtualized applications – applications that are encapsulated away from the underlying operating system – may be more easily migrated to a cloud environment, but some services and applications may never be able to migrate.

2. The Department of Defense's Approach to Cloud Computing

A. History of Cloud Computing in the Department of Defense

DoD has historically relied on on-premises DoD data centers to host applications and provide IT infrastructure. These data centers are widely dispersed across military installations and vary in management, operation, and capability. Traditional data centers suffer from slow upgrade periods and low utilization (averaging 30% utilization). (DOD CIO, 2012, p. 4) Cloud computing technology offers a way for DoD to lower costs per unit of computing resource, improve performance, and increase utilization, thereby increasing the cost efficiency of IT.

1. DoD Cloud Computing Strategy 2012–2014

In July 2012, the DoD CIO issued the DoD Cloud Computing Strategy to address some of the challenges posed by traditional data centers. This strategy laid out several steps toward delivering cloud services to the department, including:

- "Reform DoD IT financial, acquisition and contracting policy";
- "Consolidate and virtualize legacy applications and data";
- "Incorporate core cloud infrastructure into data center consolidation";
- "[Leverage] the Federal Risk and Authorization Management Program (FedRAMP)… standard approach to assess and authorize [commercial] cloud computing services";
- "Optimize the delivery of multi-provider cloud services through [an Enterprise] Cloud Service Broker." (DOD CIO, 2012, pp. E-3)

The Strategy envisioned a robust multi-provider cloud environment made up of commercial, Federal Government, and DoD-only CSOs. Commercial cloud offerings would leverage FedRAMP, the government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The Enterprise Cloud Service Broker (ECSB) would then manage the use, performance, and delivery of each CSO for the Department. Instead of each mission owner tracking and managing the CSO, the ECSB would focus on the details of the cloud implementation – cybersecurity, authentication, load balancing, and contracting – allowing the mission owner to focus on their mission. (DOD CIO, 2012, p. 18) The

DoD CIO named the Defense Information Systems Agency (DISA) as the Department's ECSB in June 2012 and required DoD components to acquire cloud computing services through the ECSB. (Takai, 2012)

During this same period, DISA developed a number of private cloud instantiations that it hosts on the DoD Information Network (DODIN), under the oversight and configuration management of the Department. These include Defense Connect Online, a web conferencing platform; DoD Enterprise Email,[1] which provides e-mail services to approximately 1.7 million users; and milCloud, a DISA-developed cloud-service portfolio. Although not mentioned by name in the Cloud Computing Strategy, milCloud was envisioned to play a central role in the DoD Enterprise Cloud Environment, which would in turn be a central piece of the Department's JIE construct. DISA built milCloud as an IaaS offering composed of commercial-off-the-shelf (COTS) and government-developed technology. DISA designed the milCloud environment to offer all the expected characteristics of cloud (e.g., on-demand self-service, resource pooling, and rapid elasticity) while residing on infrastructure housed in DoD data centers. Other private cloud applications were developed during this time.

After two years, implementation of the 2012 DoD Cloud Computing Strategy achieved limited success. Among the challenges, many organizations were concerned that DoD's approach was too slow and too bureaucratic. (Konkel, 2014) For example, by the end of 2014, six commercial CSOs had received a DoD Provisional Authorization. The DoD Inspector General reported that, two years after issuing the strategy, DoD had still not fully executed several elements of it, including training and contract reform. "As a result," the Inspector General reported, "DoD may not realize the full benefits of cloud computing such as cost savings, increased mission effectiveness, and increased cybersecurity." (Department of Defense Inspector General, 2014)

2. DoD Transition to Commercial Cloud 2014–Present

In December 2014, the DoD CIO issued a memo removing the requirement that DoD components acquire cloud services through the ECSB. Instead, they could acquire cloud services directly from DoD-approved CSPs. (Halvorsen, 2014) New investments in the cloud would need to be justified by an IT business case analysis that would ensure a consistent approach to evaluating investment options. The memo also established a requirement that commercial cloud service providers who wished to host sensitive unclassified DoD data must adhere to the newly published DoD Cloud Computing

[1] DoD Enterprise Email (DEE) is a service that DoD considers to be cloud-based. However, because of its architecture based on Microsoft Exchange servers, with users provisioned on servers based on geographic location, this service does not have all the characteristics of other cloud-based e-mail services that were developed specifically for cloud use.

Security Requirements Guide (SRG). DISA would still be responsible for validating that providers meet the baseline FedRAMP security standards as well as the additional requirements of the SRG. DISA would also remain responsible for issuing DoD Provisional Authorizations for CSOs. Finally, the memo specified that connections to public commercial cloud infrastructure would pass through authorized, DoD-managed Cloud Access Points to provide additional security. (Halvorsen, 2014)

B. DoD's Current Approach to Commercial Cloud Computing

At a March 2015 workshop on commercial cloud adoption, a DoD CIO representative summarized the new policy to mission owners with the following five-step process for acquiring cloud services:

1. Perform an IT business case analysis (BCA),
2. Apply the DoD Cloud Security Requirements Guide,
3. Use commercial cloud services that have a DoD Provisional Authorization and a Component Authority To Operate (ATO),
4. Use an approved DoD Cloud Access Point and Computer Network Defense Service Provider to protect sensitive data,
5. Apply Defense Federal Acquisition Regulation Supplement (DFARS) class deviation (and upcoming interim rule) to commercial cloud contracts.

1. IT Business Case Analysis

The DoD CIO uses an IT BCA approach to evaluate the acquisition of commercial cloud capabilities. The BCA template, which the mission owner can tailor based on the scope and complexity of the investment, is intended to facilitate a comparison of alternatives with respect to cost, benefits, operational impacts, and risks. While the DoD CIO issues the BCA template, the DoD Component CIO (i.e., the CIO of the military Department or Defense agency) reviews and approves the individual BCAs. The December 2014 DoD CIO memo requires the BCA to consider DISA-provided cloud services, such as milCloud, as an alternative to commercial offerings. (Halvorsen, 2014)

2. DoD Cloud Computing Security Requirements Guide

DISA released the DoD Cloud Computing SRG in January 2015.[2] (DISA, 2015) This document updates and supersedes the previously released Cloud Security Model, with the intent of outlining "the security controls and additional requirements necessary for using cloud-based solutions within the DoD." Controls are based on FedRAMP security controls, with additional controls specified by DoD policy for sensitive information.

A fundamental concept in the SRG is information Impact Levels, which provide a way to categorize the sensitivity of DoD data that could be stored or processed in the cloud. Four Impact Levels are in use, numbered 2, 4, 5, and 6 for historical reasons. DISA requires the FedRAMP Moderate list of required controls from NIST SP 800-53 as the bare minimum for its least sensitive data (SRG Impact Level 2). As sensitivity increases, additional control requirements from Committee on National Security Systems Instruction (CNSSI) 1253 are used for Impact Level 4 (For Official Use Only (FOUO), Personally Identifiable Information (PII), Protected Health Information (PHI), and Controlled Unclassified Information (CUI)), Impact Level 5 (National Security System and particularly sensitive CUI), and Impact Level 6 (classified up to Secret). Table 2-1 provides more information about the information Impact Levels.

Table 2-1. DoD Information Impact Levels (Source: DISA, 2015)

Information Impact Level	Description
2	Non-Controlled Unclassified Information – data cleared for public release and DoD private unclassified data not designated as controlled or critical mission data
4	Controlled Unclassified Information – data that, under law or policy, requires protection from unauthorized disclosure or is otherwise critical mission data; examples include: Personally Identifiable Information (PII), Protected Health Information (PHI), For Official Use Only (FOUO), and Export control
5	Controlled Unclassified Information – data that the data owner deems necessary to protect at a higher level; also data that supports unclassified National Security Systems
6	Classified Information up to Secret – data that has been determined to be classified national security information; note that data classified above Secret is outside the scope of the Department's current cloud efforts or the cloud SRG

[2] During the writing of this report, DISA released an updated Draft of the DoD Cloud Computing SRG in July 2015. This version modifies many sections of the January 2015 SRG and includes expanded information on classified cloud environments. As of October 2015, this new version remained in Draft. IDA recommends that interested parties review the most current SRG at: http://iase.disa.mil/cloud_security/Pages/index.aspx

The SRG specifies technical architecture requirements for CSOs, guidelines for data recovery and destruction, and Computer Network Defense (CND) requirements. The SRG also specifies physical facility and personnel requirements, including when employees of CSPs must undergo background checks.

3. DoD Provisional Authorizations

DISA describes a DoD Provisional Authorization (PA) as "an acceptance of risk based on an evaluation of the CSP's offering and the potential for risk introduced to DoD networks." (DISA, 2015, p. 8) CSPs that provide cloud offerings to DoD must have a FedRAMP PA. For CSOs hosting Impact Level 4 data and above, DoD has specific security controls and requirements (referred to as FedRAMP+), to ensure that the CSO can meet and assure DoD's critical mission requirements. Once DoD assesses a CSO in accordance with the FedRAMP+ criteria, outlined in the SRG, it awards the CSO a DoD PA. (DISA, 2015) FedRAMP PA and DoD's FedRAMP+ PA can be assessed simultaneously.

4. DoD Cloud Access Point

DISA describes a DoD Cloud Access Point (CAP) as "a system of network boundary protection and monitoring devices, otherwise known as an [information assurance (IA)] stack, through which CSP infrastructure will connect to a DoD Information Network (DoDIN) service; the Non-secure Internet Protocol Router Network (NIPRNet), or Secret Internet Protocol Router Network (SIPRNet)." (DISA, 2015, p. 45) The CAP sits as a gateway between the commercial cloud service offerings and the DoD network, protecting the DoDIN from cybersecurity vulnerabilities in the cloud, while still being permissive enough to allow application and data hosting in the cloud. The CAP is used only for connections to CSOs rated for processing data at Information Impact Level 4 and above; Level 2 CSOs connect directly to the Internet. (DISA, 2015, p. 46) A DISA official stated that DISA designed the CAP with recognition that the connection to an approved CSO is more secure than a connection to the unfiltered Internet, because approved CSOs have already gone through a comprehensive security review (either FedRAMP for Level 2 data or FedRAMP+ for Level 4/5 data).

In the first half of 2015, DISA completed and began operating its CAP. Although DoD Services and Agencies are not required to use the DISA CAP – for example, the Navy is building its own CAP – the DoD CIO wants to transition all DoD access to a DISA-provided CAP at an unspecified future point. (Halvorsen, 2014) Regardless of which organization builds and operates a CAP, the DoD CIO must approve it.

5. Contracting and Legal Concerns

DoD has issued special acquisition rules that govern the purchase of cloud computing services. DFARS Class Deviation 2015-O0011, Contracting for Cloud

Services (USD(AT&L), 2015) requires purchase requests for cloud computing services to:

- Require compliance with the DoD Cloud SRG;
- Specify data ownership, licensing, delivery, and disposition instructions;
- Contain applicable privacy impact assessment requirements;
- Set limitations for contractor access to, and use and disclosure of, Government data;
- Specify requirements to support inspection, audit, investigation, and similar activities;
- Specify requirements to respond to any spillage of classified or controlled unclassified information.

DoD further codified many of these provisions with an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) in August 2015. (Defense Acquisition Regulations System, 2015)

In addition, the DoD CIO has advised mission owners that contracts for cloud services should consider:

- Service-Level Agreements, including performance standards and enforcement mechanisms;
- Terms of Service/End-User Licenses and whether they include any clauses that the government cannot accept due to existing law or policy;
- Personnel access, especially if CSP personnel are required to have a background investigation or be U.S. persons;
- Use of subcontractors by the CSP and how that might introduce additional risk;
- Whether CSP should have cyber incident insurance to pay for costs associated with a breach of hosted DoD data;
- Geographic location of the data, and whether it must remain in the United States (Impact Level 5/6) or can be hosted internationally with approval (Impact Level 2/4).

C. MilCloud – DoD's Internal Cloud Offering

DoD continues to invest in milCloud while incorporating new commercial CSOs. The milCloud CSO from DISA is composed of two primary capabilities: the Virtual Data Center (VDC) and milCloud Orchestrator. (DISA, n.d.)

The VDC is DISA's DoD-specific IaaS cloud service offering. It is built from commercial hardware and offered to DoD customers at the Unclassified and Secret classification levels. (Martin, 2014) The operating systems offered to users include Microsoft Windows, Red Hat Enterprise Linux, and Oracle Solaris. Data storage is provided via a redundant array of inexpensive disks (RAID) that yield high reliability in the face of independent disk failures. The hardware supporting the VDC is located at the Defense Enterprise Computing Centers (DECC) located across the country. Depending on the architecture a cloud customer uses, this could be helpful in providing resilience against a failure of one or more of the DECCs.

As an IaaS offering, the VDC provides a cloud-based infrastructure. However, the mission owner is responsible for installing, maintaining, and securing the operating system and applications that they run in milCloud. DISA is responsible for the hardware (servers, routers, cabling), electricity, cooling, storage, hypervisors,[3] network, and limited aspects of the guest operating system (i.e., the one provided as a service to customers). The network traffic flows through the DISA security stack and is directly monitored by DoD, providing some additional security.

The milCloud Orchestrator assists customers in automating aspects of the VDC. Customers can automatically provision additional VDC resources, configure environments using predefined configuration settings, and run tests and scans. While VDCs enable a customer to achieve efficiencies in terms of capital expenditures for equipment, with some savings for labor, the Orchestrator focuses on achieving efficiencies primarily in terms of labor.

[3] The hypervisor is the piece of software on a physical machine that manages and separates virtual machines running on top of it.

3. Metrics for Measuring DoD's Adoption of Commercial Cloud Capabilities

Metrics enable an organization to measure progress toward a goal. They also allow an outside observer to compare similar efforts across organizations. Cloud computing is a relatively new field, and there are no widely accepted metrics for measuring cloud adoption rates or benchmarks for organizations transitioning to the cloud. Therefore, IDA developed the following broad categories of metrics that can measure DoD's cloud adoption and the value provided by commercial cloud offerings:

- Statistics for Cloud Service Offering Adoption – provides an objective measure of the availability and types of CSOs;
- Value through Cost savings/cost avoidance – provides a measure of the financial value of transitioning data and applications to a commercial cloud environment;
- Value through Usability – provides a measure of the ease with which DoD mission owners can acquire and use commercial cloud services;
- Value through Automation – provides a measure of how the cloud environment is reducing IT labor requirements for the setup and maintenance of cloud instantiations;
- Value through Availability – provides a measure of how much uptime the cloud environment is achieving;
- Value through Security and Compliance – provides a measure of the confidentiality, integrity, and availability of data in the cloud.

A. Statistics for Cloud Service Offering Adoption

The Department can measure progress in adding CSOs by simple aggregation of data about the various CSOs with DoD Provisional Authorizations. Generally, increasing numbers demonstrate progress toward cloud adoption. Recommend statistics to collect include:

- Number of approved CSOs by cloud service model (e.g., IaaS, PaaS, SaaS);
- Number of approved CSOs by cloud service model and purpose (e.g., IaaS, office productivity, customer relationship management, human resources, Linux PaaS, etc.);

- Number of approved CSOs by information Impact Level (e.g., Level 2, 4, 5, or 6);
- Number of DoD services/agencies using each CSO;
- Total number of cloud deployments across the Department;
- Number of user licenses, by CSO and in aggregate;
- Utilization of licenses, by cloud service instance and in aggregate. (Note that as opposed to normal IT acquisition, cloud services are generally billed as they are used. Therefore, utilization rates under 100% are not indicative of waste. However, higher utilization indicates higher levels of adoption.)

B. Value through Cost Savings and Cost Avoidance

One of the benefits of cloud computing is the potential to reduce the per unit cost of computing services. Services are delivered on demand, so organizations no longer have to make massive upfront infrastructure investments that may end up being underutilized. However, this same benefit makes calculating those cost savings quite difficult. With traditional IT investments, the total cost is known (or at least estimated) up front. With cloud services, the aggregate cost can change over time as usage changes. Depending on the contract agreement, the per unit cost of the cloud service may decrease over time as well, leading to savings that cannot be anticipated at the outset. For example, the CIA expects that, similar to the commercial market, the service prices of its private Amazon-provided cloud service will decrease over time as adoption increases. Cloud services may fall prey to Jevon's Paradox, which states that as technology becomes more efficient, the rate of use of that technology will increase, which leads to greater overall use and greater overall cost. (John Polimeni, 2007) As cloud computing becomes cheaper and the barriers to entry become fewer, the overall amount that the Department spends on it may rise, relative to what they might have spent on traditional IT.

Calculating cost savings or cost avoidance requires an understanding of the Total Cost of Ownership (TCO) of both the cloud service and the traditional, on-premises alternative. Savings are the difference between the TCO of the chosen solution and the TCO of the alternate solution. The majority of cloud costs are subscription costs, with subscriptions billed either per license or per unit of service cost (where unit of service is measured in computing time, number of requests processed, or megabytes stored or transferred). Cloud costs may also include implementation and training costs, especially if legacy applications are being migrated to the cloud. However, in some cases these aspects incur no additional costs if applications were originally designed for a virtualized or cloud environment.

An organization can measure traditional IT costs in capital expenditures, operating costs, and maintenance costs, which include labor costs to customize and maintain the hardware and software. Traditional IT costs include the cost of having unused IT capacity on standby as demand for an application or service grows. Traditional IT costs may also have long-term replacement costs once equipment reaches end of life (usually 5 years); those costs are invisibly integrated into cloud pricing.

Cloud computing costs are frequently more visible than on-premises costs, because the majority of cloud costs are wrapped into a known subscription fee. However, because cloud computing is billed as it is used (i.e., Pay As You Go), the aggregate amount paid for the subscription may change over time. As shown in Figure 3-1, the majority of on-premises IT costs are often hidden at the outset because they involve things like personnel and maintenance that may go beyond what is captured in a formal software license or IT management contract. Software licenses may also apply to cloud computing, depending on the type of cloud model being used (e.g., SaaS will include software licenses while IaaS may not).

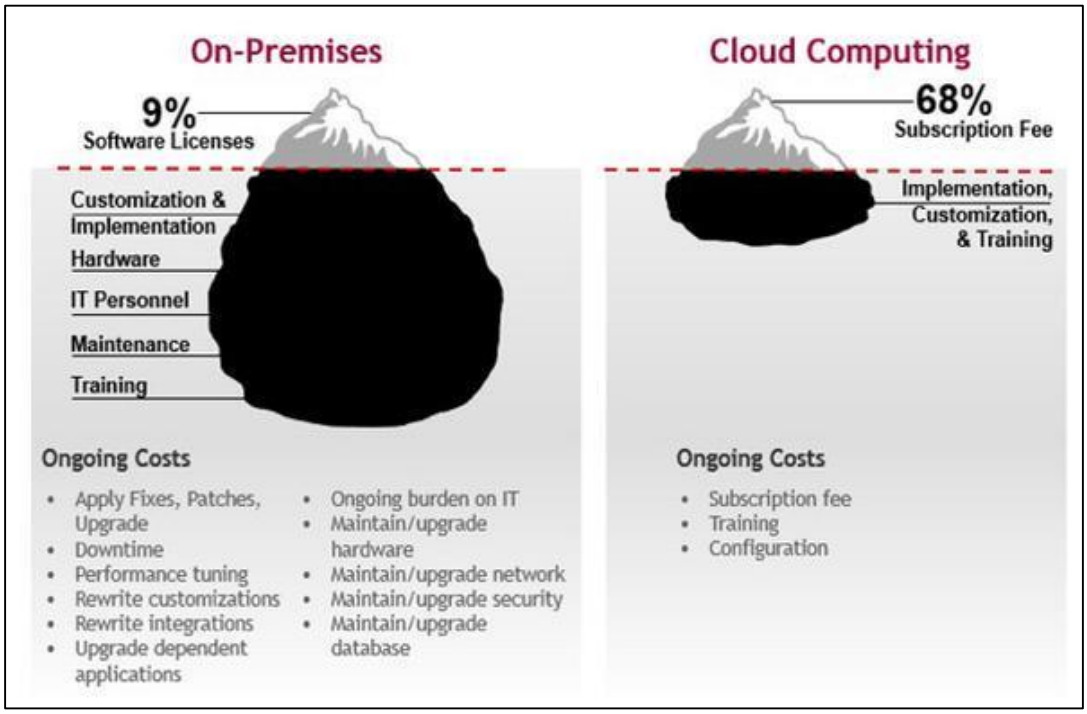

Figure 3-1. Cost Comparison of On-Premises IT and Cloud Computing (Source: Mahoney, 2014)

In addition to the TCO of the system, moving from a traditional IT infrastructure to a commercial cloud infrastructure also introduces several unanticipated avenues of cost savings and expenditures. For example, by outsourcing servers from on-premises locations to the commercial cloud, military installations can achieve significant savings in

electricity costs. (Masanet, et al., 2013) In cases in which cloud implementations have greater availability and uptime than traditional implementations, cloud computing can lead to savings through increased productivity. However, as cloud use increases, there may be a need for increased bandwidth and an upgraded network to accommodate the larger bandwidth demands, driving up network costs. Architecting applications for the cloud environment can mitigate the larger bandwidth demands. Savings may also rely on shutting down and discontinuing support for legacy equipment, which the Government Accountability Office (GAO) found the Federal Government often has difficulty doing. (GAO, 2012) Without turning off legacy equipment and applications, an organization cannot achieve the anticipated cost savings from migrating to the cloud.

As DoD begins to collect data on cost savings, it must ensure that its IT contracting and financial management data is properly aligned to the cloud Pay As You Go model. Traditional IT is usually tracked as a capital expenditure (CAPEX), while cloud computing is tracked as an operational expenditure (OPEX). In DoD budgeting, separate money may be designated for CAPEX and OPEX, so the mission owners must ensure that they align their financial tracking to their cloud strategy. In a 2015 analysis, Gartner found that "few organizations have implemented financial management processes for public cloud, and therefore few have any idea whether they are saving money." (Cancila, 2015) Gartner recommends that organizations define processes for continual financial monitoring, with appropriate alerts and triggers, so that cloud costs do not unexpectedly increase in the period between financial reviews. DoD may benefit from a centralized cost measurement function that can determine whether overall IT expenditures rise or fall as organizations adopt commercial cloud computing.

C. Value through Usability

One of DoD's goals for cloud computing is to improve usability by reducing the layers of bureaucracy that have historically impeded rapid acquisition of IT services. There are a number of ways to measure usability, but a subjective "expectation" metric is the most valuable for tracking and measuring cloud adoption. (Sauro, 2011) Users will have expectations about the difficulty of certain adoption tasks (e.g., acquiring cloud services, completing BCA templates, and migrating data). When tasks are harder than users expect them to be, DoD can invest resources to improve the process. As familiarity with the cloud increases, user expectations will change; DoD will have to improve to keep up with those expectations.

DoD can use the same approach to measure the usability of the cloud environment itself. At the Human-Computer Interaction (HCI) International 2015 conference, NIST employees proposed the usability requirements for cloud instantiations, shown in Figure 3-2.

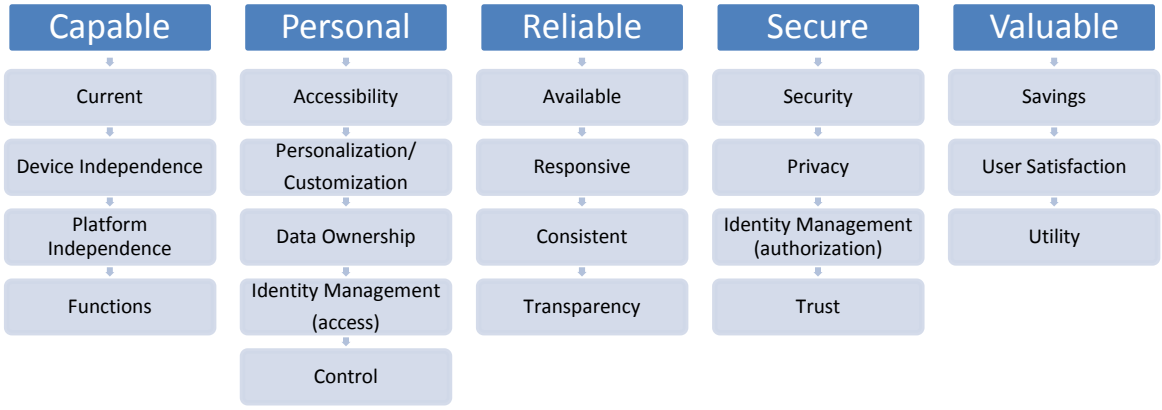

Figure 3-2. Consumer Expectations of the Cloud (Source: Stanton, Theofanos, & Joshi, 2015)

DoD can use an expectation matrix to rate the usability of each CSO in these areas. While some items overlap with other proposed metrics (e.g., Cost Savings, Availability), all figure into the overall user experience. At a minimum, the cloud environment should have the same usability rating as the traditional IT services it is replacing.

Data collection and analysis for this metric can be difficult because it is based on aggregated user expectation and opinion. One approach to collection would be to use an interstitial page or pop-up after a task is completed (e.g., "Before you leave, rate how easy this was on a scale of 1–10"). Another approach would be to survey a random sample of users, to understand their experiences. However, depending on the measured task, it could be difficult to collect a statistically valid number of responses that could track improvement.

D. Value through Automation

One of the defining features of cloud computing is automatic provisioning of services and capabilities without human interaction. For example, the cloud environment should be able to automatically create server instances, acquire additional storage capacity, or shut down services that consumers no longer need. DoD should measure how well cloud service providers are implementing automation, and ensure that its own business processes (e.g., procurement rules, paperwork requirements) are designed to take advantage of an automated environment.

In order to measure automation, DoD should review CSOs and rate the capabilities of any self-service portals or automatic capacity adjustment services that they offer. For example, CSOs that host websites should automatically provision extra capacity if demand for that website increases; if they do not have this capability, they would receive

a lower score. Mission owners should receive aggregate automation scores so that they can better understand the CSO capabilities. DoD should also identify all the steps in a given cloud computing business process and count how many of those steps require human intervention. Over time, DoD can track these processes to see how CSOs are leveraging automation to improve task speeds. Data collection is not difficult, but it does require detailed understanding of the cloud processes.

E. Value through Availability

Availability is the uptime and accessibility of an IT offering. Availability is a key performance parameter for an information system, but it can often be overlooked in cloud instantiations because the cloud is assumed to be always "up." In actuality, commercial CSOs should be carefully examined to make sure that their availability meets mission requirements and exceeds what can be achieved in DoD data centers. CSOs can be measured on the following metrics:

- Percentage of uptime,
- Number of partial outages plus percentage of time partially out (e.g., three partial outages, representing .01% of total time),
- Number of total outages plus percentage of time completely out,
- Service Level Agreement (SLA) requirements (e.g., requires 99.9% uptime to restore),
- SLA violations (e.g., two instances of restoration time being longer the allowed time to restore).

In establishing and tracking these metrics, there should be a good-faith effort to ensure that individuals use terms consistently across CSPs and DoD data centers. For example, some organizations only treat unscheduled downtime as "downtime" when they report on it, while others view all downtime – scheduled and unscheduled – as reportable.

F. Value through Security and Compliance

Measuring the security of an information system is difficult, because unknown vulnerabilities and undetected network intrusions can exist in what appears to be a secure system. Therefore, experts frequently measure the security of information systems through a certification process, in which a third party assesses the information system for compliance with a set of security controls. If technology providers achieve compliance with security controls, there may still be security incidents but those incidents are more likely to be detected and mitigated.

The Federal Government's FedRAMP program and the DoD FedRAMP+ assessments perform the compliance check on CSOs that are interested in hosting DoD

data. Each CSO is unique, and it is difficult to compare the end-to-end time required to review and certify each offering. However, DoD can track the parts of the process that are common for every CSO, such as the intake and processing of templates. Faster processing is beneficial to both the government and the commercial cloud providers. However, it is important that the thoroughness of the security review process be maintained and not sacrificed for speed.

The United States Computer Emergency Response Team (US-CERT) defines a security incident as an occurrence that "constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." (NICCS, n.d.) When security incidents occur, it is important to investigate the timeline of the incident, identify the root cause, and develop a remediation strategy. By doing so, DoD can track:

- The number of incidents across CSOs that result in loss of confidentiality, integrity, or availability;
- The percentage of time the CSO was internally known to be in a vulnerable or non-compliant state;
- The speed and thoroughness of incident response activities, measured against the requirements defined in the CSO service-level agreement:
  - The time between incident and government notification,
  - Automated courses of action used.

These metrics will help mission owners make more-informed decisions about which CSOs most appropriately meet their mission's risk profile.

4. DoD Progress in Adopting the Commercial Cloud

DoD is in the early stages of integrating the commercial cloud into its computing model. Since December 2014, DoD has made significant progress in issuing Provisional Authorizations (PA) for commercial CSOs. However, DoD has authorized the majority of CSOs to process data no higher than Impact Level 2, limiting the ability of mission owners to use the cloud for anything other than non-sensitive DoD data and applications. DoD mission owners are moving data and applications to commercial cloud offerings, but as of October 2015, many of these transitions are still in progress or in a pilot phase. There are also numerous other opportunities for transitions to the cloud. Overall, DoD is making progress toward adopting commercial cloud, but it can do more.

A. DoD Commercial Cloud Service Offerings and Uses

As of October 1, 2015, DoD lists 32 commercial cloud offerings with DoD PAs. These offerings are spread across 22 CSPs. Figure 4-1 shows the distribution of service models – IaaS, PaaS, and SaaS – across the commercial cloud offerings. (DISA, 2015)

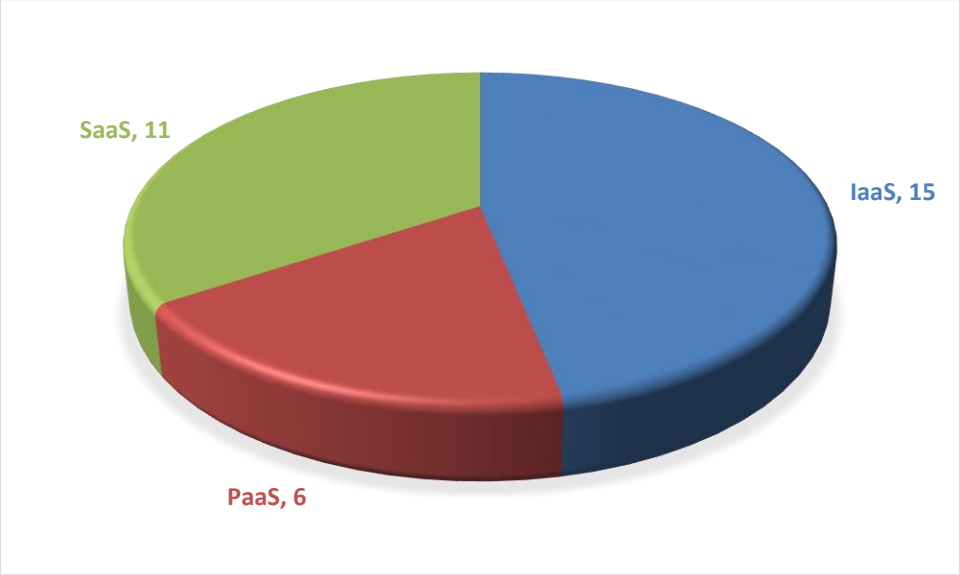

Figure 4-1. DoD Commercial Cloud Offering by Service Model (Source: DISA)

Figure 4-2 shows the distribution of CSOs by information Impact Level. Two CSOs are approved for Impact Level 4 data; the remaining 30 are approved for Impact Level 2. Fourteen CSOs are in the approval pipeline for Impact Level 4, and 4 CSOs are being processed for Impact Level 5, giving hope for additional high-sensitivity CSOs in the near future.

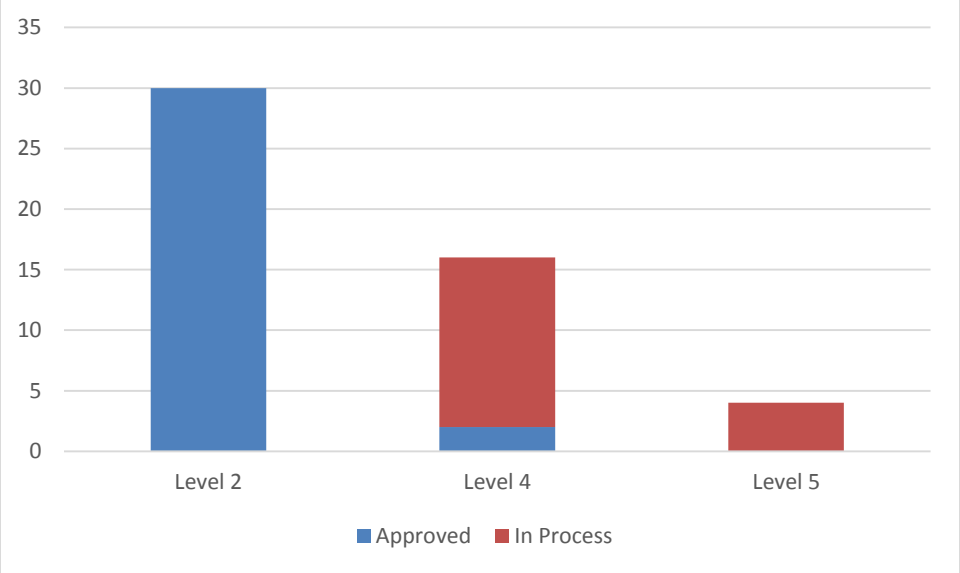

Figure 4-2. CSOs Approved and In Process by Information Impact Level (Source: DoD CIO)

There are 28 deployments of commercial CSOs within DoD, divided among eight different Defense services and agencies. Figure 4-3 shows the breakdown of DoD commercial cloud deployments by service and agency.

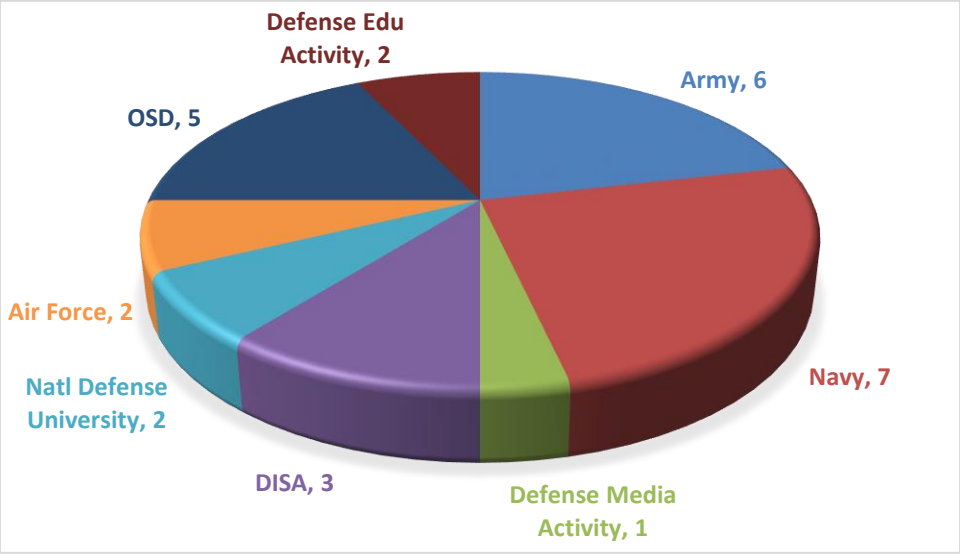

Figure 4-3. Use of Commercial Cloud by DoD Service and Agency (Source: DoD CIO)

The 28 deployments are divided among 12 CSOs, listed in Table 4-1. These CSOs correspond to nine CSPs; some CSPs (e.g., Amazon, Google, and Microsoft) have multiple offerings. Some of the piloted cloud services existed prior to the change in strategy laid out in the DoD CIO's memo of December 2014; therefore, not all of the listed CSOs are operating with DoD PAs and instead have component-issued authority to operate. It is unclear how long DoD will continue to allow CSOs without DoD PAs to support DoD missions.

Table 4-1. Commercial Cloud Service Offerings Currently in Use by DoD

Cloud Service Provider/Offering	DoD PA Level	Number of Deployments
Akamai		
Content Delivery Service	Level 2	1
Amazon		
AWS East/West	Level 2 (Level 4 in process)	1
AWS GovCloud	Level 4	12
Blackboard		
Blackboard Learning Management System	None	2
BOX		
BOX	None (Level 4 in process)	1
Google		
Google Apps for Education	None	2
Google Apps for Gov	None	1
IBM		
IBM Cloud Services	Level 2	1
Microsoft		
MS Office 365	Level 2	1
MS Office 365 Dedicated with International Traffic in Arms Regulations (ITAR) Support	Level 2 (Level 5 in process)	1
Oracle		
Oracle Service Cloud	Level 4	4
Schoology		
Schoology Learning Management System	None	1
Total Cloud Service Offerings in Use		**28**

DoD has not yet made an enterprise-wide effort to estimate cost savings or cost avoidance from using commercial cloud providers. The DoD CIO has stated that each mission owner will ultimately be responsible for reporting savings and cost avoidance attributable to commercial cloud use, measured against the IT BCA used to select the CSO. In the future, aggregation of this reported information will be available. Mission

owners will need to be careful when representing savings due to server and application rationalization and data center consolidation, in order to avoid misinformation.

B. Choice of Cloud Service Model

The most commonly offered cloud service model is IaaS, and the most frequently chosen CSO is Amazon GovCloud, which DoD categorizes as an IaaS offering.[4] IaaS allows a high level of flexibility for the customer, but it is up to the customer to configure their applications accordingly. Many of the benefits of the cloud (e.g., rapid scaling due to demand, distributed computing that is fault-tolerant) are only possible when applications are specifically designed to work in a cloud environment and integrate with the cloud orchestration capabilities. This requires mission owners to have a cloud-literate IT workforce to design, install, and configure the applications.

As cloud services expand, IDA anticipates that DoD mission owners will rely more on SaaS offerings. SaaS allows rapid integration of work products, competitive licensing, and analytical tools that are unavailable with standalone software packages. SaaS also provides the complete cloud solution to mission owners, permitting them to focus on their missions and not their IT implementations. For example, in July 2015, the Air Force and the Defense Logistics Agency (DLA) announced that they would transition to a 100,000-seat contract for a tailored version of Microsoft's productivity suite SaaS offering, Office 365. (Pomerleau, 2015)

C. Speed of DoD's Commercial Cloud Adoption

DoD's move to commercial cloud computing can be described as being a "fast follower." Fast followers are not as quick to incorporate new technologies as "early adopters," but they avoid much of the risk associated with using unproven technologies. Fast followers are also better positioned to develop a long-term strategy around a technology because they can gauge demand for the technology and understand more of its enduring uses. The downside of fast followers is that their later entry into the consumer market makes them slower to reap the efficiency rewards made available by new technologies. (Blank, 2010) Figure 4-4 shows where fast followers sit in the technology adoption life cycle.

[4] Amazon GovCloud has properties that could be considered PaaS as well as IaaS. For purposes of this analysis, IDA deferred to the DoD categorization.

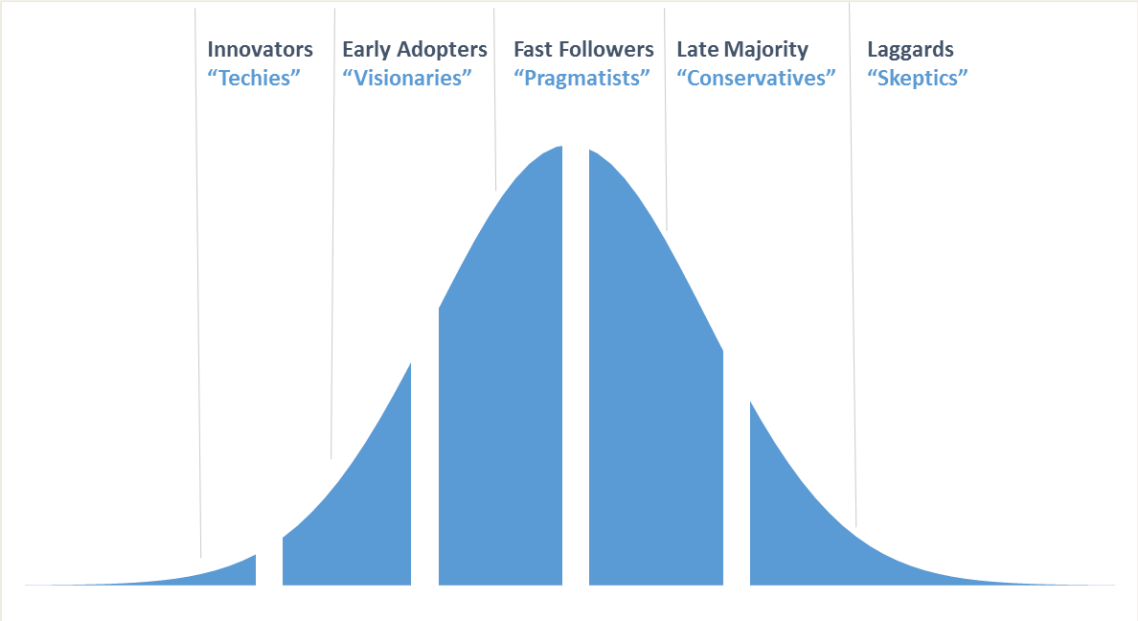

Figure 4-4. Technology Adoption Life Cycle (Source: Adapted from Moore, 2014)

The fast follower approach is appropriate given DoD's overall risk profile. DoD's missions require proven, dependable information systems that are less susceptible to cybersecurity risk. The loss of confidentiality, integrity, or availability of DoD systems can put lives at risk. Cloud computing has improved dramatically over the last decade, but it has only become widely adopted by industry and government since 2010. Now that other Federal organizations with more risk tolerance have proven the value and capability of cloud service offerings, the time is right for DoD to move many of its applications and data storage systems to the cloud.

DoD's fast follower approach also allows it to move toward a diversified portfolio of cloud service providers and offerings. DoD's approved list of offerings includes multiple large and small vendors, some of whom may not have existed when cloud technologies were maturing in the commercial space. By allowing the market to mature, DoD mission owners are not locked in to any single vendor or government-provided solution. Multiple vendors can lead to a greater variety of solutions and more competition on price, creating better cloud offerings for the Department. Since all vendors go through the same security certification process, there is limited cybersecurity risk of choosing one vendor over another.

However, DoD's approach to its diversified portfolio may introduce some performance risk. With 32 vendors currently offering solutions, and an additional 18 in the process of security approval, DoD may be diluting the market from which its mission owners must choose. Some CSOs will inherently perform better than others, be easier to

use, or provide more support to their customers. Right now, there is no way for mission owners to evaluate the CSOs, other than through an intense selection process.

DoD could improve its approach by culling out commercial cloud service offerings that do not meet a specified basic set of performance standards. A refined set of CSO options would allow qualified high potential candidates to rise to the top while reducing the government time and effort needed to evaluate inappropriate entrants. This approach would also help application and service developers to target a smaller number of cloud platforms for its government users, enabling small and innovative business engagement. For example, the CIA successfully used a source selection process that augmented the traditional proposal process with verification of features and live use case demonstrations by offerors (a.k.a. oral solicitations).

Not every major CSP business model aligns with the DoD marketplace. Some CSPs may not want to adhere to the DoD security guidelines, instead adopting a less customizable approach (e.g., security control incongruencies). Now that the cloud is a more disruptive and mature technology, DoD has more choices in vendors and can instead work with partners that understand and can adapt to the unique DoD mission environment and requirements.

D. Determining What DoD Data and Applications Belong in the Cloud

The Department has provided some guidance on what information should first be migrated to the cloud. For example, the Cloud Computing SRG encourages the migration of publicly available information to the cloud. However, DoD could do more to provide detailed guidance on migration of sensitive information. For example, critical defense-related information that describes sensitive design information for weapons and information systems should remain in DoD data centers or with the system manufacturer in the short term. This data and other data related to the DoD "crown jewels" whose loss would compromise warfighter mission effectiveness may be too valuable to immediately place in a commercial cloud environment. While systems authorized for Impact Level 5 *can* host such information, it does not mean that the commercial cloud is an appropriate venue yet.

DoD data centers are not inherently more secure than commercial cloud offerings. Most are likely equivalent, and depending on architecture, configuration, patching, and staff's technical expertise, the shared cloud environment may be even more secure than some government data centers. However, moving to the shared cloud environment cedes control of the security apparatus to the vendor and reduces DoD's capability for logging, monitoring, and conducting security audits of network traffic. While DoD has specified a set of security controls it believes are necessary to protect that information, these controls have not yet been tested in a real-world environment. Until more real-world testing takes place, mission owners should remain cautious.

Official guidance would provide mission owners with a context for their mission risk profiles as they determine whether the potential cost savings of the commercial cloud justifies any increased risk. Guidance could also provide an overall DoD perspective for what belongs in the cloud, recognizing that it is ultimately up to the mission owner to decide how to protect their systems and data. A useful vehicle for such guidance would be the "Best Practices Guide for DoD Cloud Mission Owners," released August 2015 by the DoD CIO. (DISA, 2015) The current version of this document focuses on the technical integration of CSOs into the DoD environment, but does not specify which data and applications would be the best cloud candidates. Absent more concrete guidance, DoD mission owners should first focus on cloud migrations of publicly available information (Impact Level 2 information), back office functions (e.g., human resources, accounting, contracting, travel), and non-critical data repositories.

E. Transitioning Legacy Applications to the Cloud

Cloud computing is only as useful as the applications that run on it, and the origins of those applications can have a significant impact on their capabilities. A 2015 survey found that 57% of DoD cloud-based applications were migrated from legacy applications, while the remaining 43% were developed in the cloud. (Hunter, 2015) When deciding to move to the cloud, DoD mission owners must carefully consider the technical costs and risks of porting existing applications and databases into a cloud environment versus building a new cloud-born application at the end of the existing application's lifecycle.

In many cases, legacy applications can move to an IaaS or a PaaS cloud environment as long as the CSO supports the operating system in which an application was developed. However, if the supported applications are not configured to take advantage of the native features of the cloud, such as elasticity and resource sharing, they may not function well. (Wexler, 2015) Legacy applications, especially those designed prior to 2005, were likely designed to run on a single server, not on multiple shared and redundant cloud servers, and they may need to be rewritten to account for scenarios such as one of the host servers going offline. Depending on the complexity of the application, the rewriting or reconfiguration may take time, money, and personnel resources that the mission owner may not be willing to spend.

Conversely, DoD mission owners looking to develop new applications or meet new mission needs should consider cloud-born applications. Cloud-born software is designed to run in the cloud and exploit the services and capabilities inherent to the cloud environment. (Telford, 2012) Cloud-born software may be SaaS, or it may be more traditional software intended to run on PaaS or IaaS instantiations. It is more likely to leverage the inherent resiliency and availability of the cloud and to support a multi-user model. The downside of mission owners insisting on cloud-born applications is that

cloud-born software development is still an emerging skillset that may be difficult to contract.

As mission owners look to transition applications to the cloud, the Department must look at its IT workforce as a whole to ensure that they have the appropriate training and mindset to take advantage of cloud technologies. Several DoD officials reported that much of the IT workforce at DISA and in the Services and Agencies still maintains a "data center-centric" mentality, with a preference for building IT capacity in house. The 2015 MeriTalk survey of DoD IT managers and staff found that the staff had a greater preference than the managers did for keeping and refactoring existing legacy applications. (Hunter, 2015) The Department is currently working with the Defense Acquisition University to develop a Cloud Learning Module, which it hopes can help educate technical staff about implementing the cloud environment.

Reliance on commercial cloud will off-load many of the technical duties currently performed by the government IT workforce, so the workforce may have understandable concerns about the effect of cloud computing on their jobs. However, a robust commercial cloud environment will still require technical oversight, and it will give existing IT staff the opportunity to focus on other duties. DoD can make the cloud a more compelling option by hiring IT professionals with experience in implementing or developing software in cloud environments.

F. MilCloud as an Alternative to Commercial Cloud Offerings

As of October 2015, DISA reports 57 mission partners operating 69 projects on MilCloud. The biggest users, in terms of computation used, are the Defense Logistics Agency, the Air Force, and DISA.

In the case of Impact Level 4 and 5 applications and data, the need for control and a high level of security often supersedes the desire to achieve high efficiencies. In these cases, milCloud may be an appropriate choice that marries many cloud capabilities with DoD in-house security. DoD can easily integrate milCloud with its existing security stack and even utilize classified knowledge and indicators of adversaries' tactics, techniques, and procedures (TTP) to identify attempts to compromise DoD resources. This is more difficult to do in shared or commercial environments, in which DoD may not be legally able to monitor such traffic. In addition, because milCloud is owned and operated by DoD, users can achieve visibility into its inner workings and supply chain, which is difficult to achieve with commercial cloud providers.

There is not a one-to-one correspondence between the provided services, offerings, and capabilities of milCloud and those of commercial CSOs. Therefore, cost comparisons can only be estimated. Prices of commercial CSOs are also fluid and scale with use, while milCloud prices are fixed and determined for each Fiscal Year. MilCloud and many

commercial vendors offer online calculators that allow mission owners to estimate their costs, based on given scenarios. Table 4-1 shows example scenarios based on virtual hardware configuration, but they do not account for services that differentiate milCloud and the commercial providers.

Table 4-2. Cost Comparison Between milCloud and Commercial CSPs*

Scenario	milCloud	Commercial CSP A	Commercial CSP B
IaaS – 2 CPU, 4 GB RAM, No Storage (per Month)	$228	$38	$119
IaaS – 8 CPU, 30GB RAM, 160 GB Storage (per Month)	$1230	$389	$833
Standard Storage (per GB/Month)	$0.46	$0.03	$0.02-$0.06

* Cost comparison is estimated and does not take into account differences in services or capabilities.

MilCloud is often viewed as an expensive alternative to commercial CSOs, with milCloud monthly costs two to ten times higher than commercial costs for similar scenarios. However, DISA officials stated that DoD does not consider milCloud to be a direct competitor with the commercial cloud. Technical expertise, business acumen, and commercial procurement practices enable a commercial cloud environment to provide more services, faster, and at lower cost than a DoD-grown cloud environment. Instead, in cases in which a desire for DoD control and security trumps a desire for lower costs, milCloud is more a competitor to DoD-owned and operated non-cloud solutions, such as standalone data centers.

Some industry officials also do not view industry offerings as competing with milCloud, but for slightly different reasons. Industry offerings are much more feature-rich than those provided currently by DISA. While milCloud provides a basic hosting environment, storage, and cloud orchestration services, this is just a fraction of the IaaS capabilities provided by commercial competitors, who provide support for containers (an alternative to virtual machines), multiple levels of storage (e.g., traditional storage versus long-term archival), hardware security modules (HSM) (used for secure cryptographic key storage), and more. Industry also offers PaaS and SaaS solutions, and DISA does not.

One capability that milCloud offers is a classified cloud service over the SIPRNet. Approximately 25% of milCloud projects operate on SIPRNet. MilCloud's SIPRNet offering allows mission owners to leverage cloud capabilities for Secret data with increased assurance about its security. The offering also allows application programmers to develop and test new capabilities in the unclassified milCloud environment, and then

transition them to the classified production environment. There are currently no planned commercial offerings for DoD Secret data (information Impact Level 6). DoD should consider whether a classified commercial offering would be of value and, if so, how to encourage the development of one. DoD should join forces and share knowledge with other security-focused Federal agencies with similar requirements and with appropriate industry partners.

G. Commercial Cloud and the Joint Information Environment

The JIE refers to a wide-ranging vision for the future of the Department's computing environment. It is intended to enable "more effective, more secure… information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure at the enterprise level." (DISA, 2014) JIE addresses a host of IT issues, including security, mobility, enterprise services, and a unified architecture. The Department envisions cloud computing, both through commercial cloud providers and through milCloud, to be a key component of the JIE. (Pellerin, 2015)

Many of the goals of JIE align with the defining tenants of cloud computing. For example, the Department plans for the JIE to enable device-agnostic access to data from anywhere. This goal matches the cloud computing concept of broad network access, which permits access to data from any authorized device. In addition, as the Department transitions to the JIE, one of its major goals is to consolidate DoD data centers. Data center consolidation can be an effective way to reduce costs and improve efficiency. The consolidation process can also create an opportunity to migrate existing data and applications to commercial cloud providers, especially if mission owners have already virtualized the data or applications.

DISA is responsible for the technical aspects of JIE and, until December 2014, it was also responsible for brokering cloud service agreements for the Department. The DoD CIO decision to transition DISA from that role and allow mission owners to contract directly with approved commercial cloud providers has many benefits, but it reduces DISA's oversight of the technical implementation and use of CSOs. As the department changes its approach to commercial cloud providers, it should update its JIE planning and strategy artifacts to reflect these changes. For example, many of the JIE strategic documents still reference DISA as the Enterprise Cloud Service Broker. To prevent future confusion, DISA should formally adjust its JIE planning and risk management strategies to acknowledge the changes in its cloud responsibilities.

5. Approving and Securing Commercial Cloud Service Offerings

A. Overview of FedRAMP

FedRAMP was created to validate the security requirements of commercial cloud offerings for the entire Federal Government. As such, its process is flexible and meant to accommodate the needs of multiple departments and agencies. Initial submittal of a CSO to the FedRAMP process can be initiated by the vendor (in this case, the vendor does not have a contract but is positioning itself for selection by a government agency) or by an Agency (in this case, the vendor has already been reviewed by the agency and is looking for FedRAMP approval).

The vendor first presents a system security plan for review by the Joint Authorization Board (JAB) consisting of security experts from the Department of Homeland Security (DHS), DoD, and the General Services Administration (GSA). The vendor addresses any JAB concerns. Government representatives have stated that in some cases, CSOs were not fully compliant with FedRAMP requirements at the outset, and the evaluation and provisional authorization process identified outstanding vulnerabilities that were remediated prior to the issuance of a PA. This provides some evidence that FedRAMP is a useful process for baselining and potentially increasing the security of cloud service offerings.

FedRAMP currently has Low and Moderate security baselines, with plans for a High security baseline. These baselines correspond to the minimum information security requirements for the information system hosted in the cloud. Each baseline consists of, among other things, a set of the NIST SP 800-53 controls that are considered mandatory for systems at that level. All of the four DISA impact levels begin with the FedRAMP Moderate baseline and add additional controls from NIST SP 800-53. As sensitivity increases, additional control requirements from CNSSI 1253 are used for Impact Level 4 and Impact Level 5.

While it might seem like overkill to require FedRAMP Moderate for public information rather than FedRAMP Low, it makes sense in the context of DoD needs. For example, consider the official DoD Press Releases page.[5] While there is no need for the data on this page to be confidential, there is a requirement for complete data integrity.

[5] http://www.defense.gov/releases/

Fake press releases could stoke fear among the public or damage alliances with other nations. Due to the high stakes of the press releases, it is reasonable to levy additional security control requirements to minimize the likelihood of an adversary injecting false data into the news stream.

B. DoD's FedRAMP+ Controls

DoD extends the FedRAMP controls in the Cloud Computing SRG with what it refers to as FedRAMP+. A significant concern for industry is that a system built for FedRAMP provisional authorization for use by the Federal Government at large may not meet all the requirements for use by DoD. This leads either to additional costs to bring the entire system up to DoD standards, with costs spread among all customers or to the creation of a separate cloud service offering for just the DoD community. In addition, commercial cloud providers questioned whether the additional security controls and isolation requirements might not be truly necessary. Mr. Matthew Goodrich, director of FedRAMP, was supportive of DoD's additional requirements, noting that the security of many DoD systems put lives on the line. In cases like this, it made sense to defer to DoD on its specific needs rather than require DoD to follow a one-size-fits-all approach.

However, there are opportunities to streamline the FedRAMP and DoD processes. As FedRAMP and the DISA Cloud Computing SRG mature, it is likely that a greater understanding of cloud security needs will result in more harmonization of requirements between FedRAMP and FedRAMP+. Controls that are seen as being particularly helpful would be brought from FedRAMP+ into FedRAMP, and those that provide little additional security at a greater cost could be removed from FedRAMP+. This is likely to result in a minimization of the difference between the two as time progresses.

C. Common Cloud Service Stack

The Cloud Computing SRG requires CSPs to adhere to specific controls that are implemented to DoD standards. The DoD CIO and DISA have recently recognized that, in addition to specified controls, commercial CSPs would benefit from the implementation of DoD-specific security services that all CSPs could leverage. As of July 2015, this is only a proposed development, but its implementation would help spur cloud adoption and ease integration of CSPs into the DoD security framework.

For example, DoD relies on a Public Key Infrastructure (PKI) model to authenticate users on e-mail and at their workstations. Instead of forcing each CSP to implement a compatible version of the PKI architecture, DoD could develop a common PKI system that the CSPs could access and leverage. Similarly, DoD could configure special malware and vulnerability scanning software for use across all participating CSPs so that CSPs would not be solely responsible for ensuring their own software security. DoD requires extensive continuous monitoring controls for CSOs hosting information at Impact Levels

5 and 6, and common services could collect and aggregate this monitoring data. Common services are planned to extend beyond security services and include IT management services, such as System Log Management and Software Key Management. Services purchased from outside vendors may have to be re-licensed or reconfigured to operate in a cloud environment. Overall, this is an avenue that is worth DoD's pursuing because it will help encourage DoD and commercial cloud provider collaboration while achieving the Department's security goals.

D. Physical Isolation of CSOs for Impact Level 5 Data

The Cloud Computing SRG lays out requirements for separation of data at the various Impact Levels. The CSP "must provide evidence of strong virtual separation controls and monitoring" for Impact Level 2 and 4 information. Dedicated physical infrastructure is required for Impact Levels 5 and 6, with Level 5 data restricted to "only DoD private, DoD community or Federal Government community clouds." (DISA, 2015) Additionally, the Cloud SRG places limitations and requirements for off-premises connectivity at Impact Levels 4, 5, and 6.

Cloud isolation requirements are a major issue that industry has raised about the DISA Cloud Computing SRG, especially with respect to Impact Level 5. The requirements for a separated physical infrastructure almost demand the build-out of a private cloud for DoD purposes, which limits opportunities for resource pooling and may be too costly to make business sense for the CSP. The SRG states that DoD will accept "alternative solutions that provide equivalent security" to the separation requirements, but industry partners report that DoD has not yet made clear how to demonstrate that equivalent security. (DISA, 2015)

DoD acknowledges that it is taking a cautious approach with respect to physical separation for Level 5 data. The reason for the isolation is that virtual machine separation can be compromised, allowing an adversary to move from one cloud tenant's systems to another tenant's systems. VENOM is a recent example of this type of vulnerability. According to security firm Symantec, "The VENOM bug could potentially allow an attacker to steal sensitive data on any of the virtual machines on this system and gain elevated access to the host's local network and its systems." (Symantec Security Response, 2015) This vulnerability makes it clear that isolation requirements make good sense; however, a better question is whether the current requirements strike the right balance for isolation.

Data separation can be implemented by either maintaining data in separate data stores or separating sensitive data from less sensitive data within the same data store. While the latter method might be more granular, the former method is likely to be simpler to achieve and more effective. The degree of separation can be defined as follows:

- **Distinct.** The user is able to distinguish one type of data from another in the same environment, such as a single cloud instantiation. Sensitive data is tagged or marked so that it can be identified as such, but it easily co-mingles with other data. Securing this data relies on robust monitoring, well-behaved systems, and mature processes.
- **Isolated.** Data is pre-sorted in advance; there is no need to distinguish between two different types because they are in separate environments. Sensitive data is kept separate from other data. It does not have an opportunity to co-mingle. Compromised systems are limited in their ability to exfiltrate data.

The methods for data separation can be defined as follows:

- **Logical.** Logical mechanisms are entirely mediated via software (e.g., software tags data by owner to identify data and keep it separate).
- **Physical.** Physical mechanisms use separate physical instances of hardware to keep data separate (e.g., separate servers support separate instantiations).

By combining the degree of separation with the methods for separation, we get the data separation mechanisms shown in Figure 5-1.

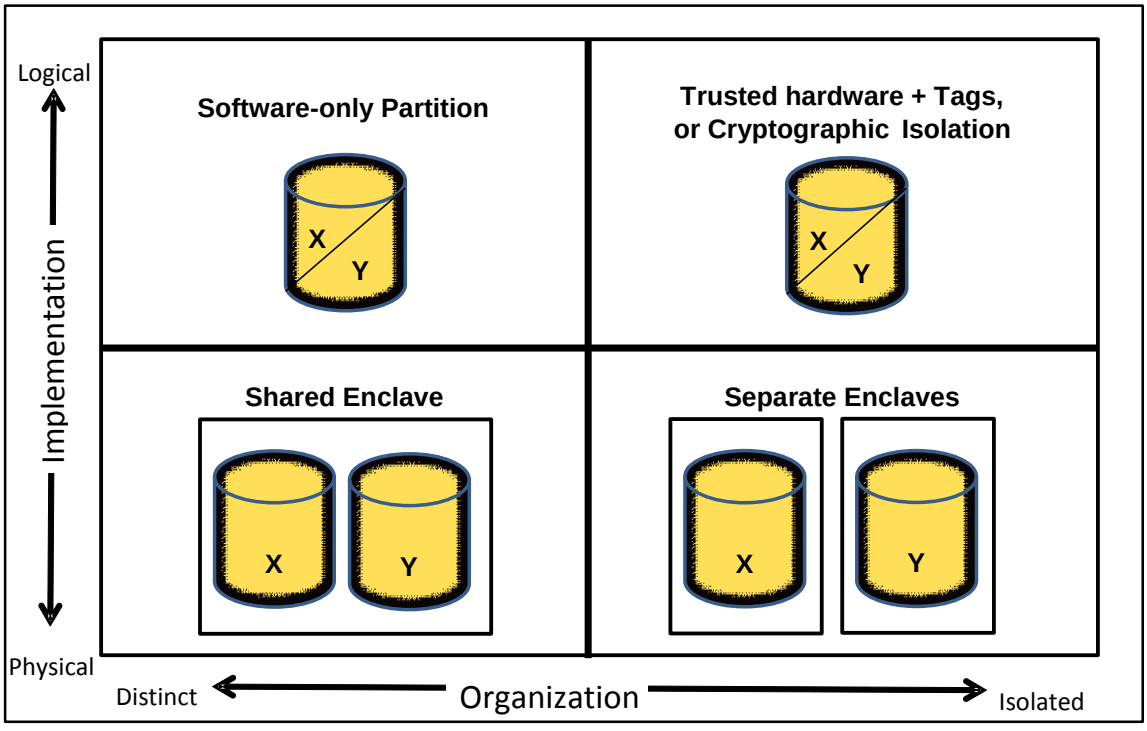

Figure 5-1. Data Separation Model (Source: IDA)

As written, the DISA Cloud Computing SRG isolation requirements allow DoD data to be co-located in a cloud with Department of Education or Department of Agriculture

data (a shared enclave), but not with defense industrial base (DIB) contractor-held data (a separate enclave). Other Federal Government partners generally do not have the same stringent requirements for data security and might be unwilling to share the services that DoD requires. DIB contractors, on the other hand, hold data that is sometimes of very high value to DoD and already must comply with security and IT requirements established by DoD. Therefore, it may make more sense to allow DIB partners to share cloud infrastructure with DoD. Allowing DIB partners and DoD to exist in the same community cloud would raise the security of the commercially held sensitive data while still ensuring that the DoD systems were co-located with security peers.

One possible way to separate the DIB partners from the DoD cloud infrastructure for Level 5 data is to allow for monitoring and protection of government network traffic while avoiding the inadvertent interception of non-government traffic. CSPs could mitigate this through logical isolation mechanisms (e.g., virtual machines, virtual local area networks (VLAN), software-defined networks (SDN), etc.) that could separate government and non-government systems without the rigid and expensive physical isolation currently required. This would still meet the spirit of attempting to avoid inadvertent monitoring of non-government communications while containing costs and enabling robust monitoring of government communications.

We recommend that future iterations of the DoD Cloud Computing SRG explore alternatives such as these to raise the protection of sensitive DIB data while allowing CSPs to achieve economies of scale by including other DoD community members to co-locate in Impact Level 5 cloud environments.

6. Conclusion

Cloud computing engenders a constant tension among IT performance, cost, and risk. It represents a new way to scale computing, realize efficiencies, and transform the purchase of IT. At the same time, its shared computing model introduces new security concerns about the confidentiality and integrity of data, and the nature of the commercial cloud cedes implementation details to an outside party.

This change is significant to the highly regimented and controlled DoD IT environment. Cloud computing requires new ways of architecting solutions, new financial tracking mechanisms, and new expectations about the speed of delivering IT solutions. Rapid provisioning of cloud resources is incompatible with a business-as-usual approach. At the same time, cloud computing requires an IT workforce who is familiar with and excited about cloud computing, and who can translate the benefits to DoD mission owners.

Despite many hurdles, DoD is making demonstrable progress in providing commercial cloud service offerings to its mission owners. As more mission owners take advantage of those offerings, the Department will begin to realize measurable efficiencies in IT performance and cost. Mission owners should focus on adopting cloud-born software and moving non-mission-essential functions and data into the cloud first, in order to better understand and gain comfort with the cloud environment. Only then should DoD begin transitioning sensitive applications and data into approved Impact Level 5 cloud service offerings that have appropriate isolation controls.

References

Abdul. (2013, October 17). *Cloud Computing Bottleneck: The Bandwidth Problem*. Retrieved from CloudTweaks: http://cloudtweaks.com/2013/10/cloud-computing-bottleneck-the-bandwidth-problem/

Barr, J. (2014, March 26). *AWS Price Reduction #42 – EC2, S3, RDS, ElastiCache, and Elastic MapReduce*. Retrieved from AWS Official Blog: https://aws.amazon.com/blogs/aws/aws-price-reduction-42-ec2-s3-rds-elasticache-and-elastic-mapreduce/

Bartles, A., Rymer, J., & Staten, J. (2014). *The Public Cloud Market Is Now in Hypergrowth.* Cambridge, MA: Forrester Research, Inc.

Benson, P. (2013, May 20). *The Cloud Defined: Measured Service*. Retrieved from PBenson.net: http://www.pbenson.net/2013/05/the-cloud-defined-part-5-of-8-measured-service/

Benson, P. (2013, May 6). *The Cloud Defined: Resource Pooling*. Retrieved from PBenson.net: http://www.pbenson.net/2013/05/the-cloud-defined-part-3-of-8-resource-pooling/

Blank, S. (2010, October 5). *You're Better Off Being A Fast Follower Than An Originator*. Retrieved from Business Insider: http://www.businessinsider.com/youre-better-off-being-a-fast-follower-than-an-originator-2010-10

Bright, P. (2013, September 17). *Meeting the bandwidth demands of taking your business into the cloud*. Retrieved from Ars Technica: http://arstechnica.com/information-technology/2013/09/meeting-the-bandwidth-demands-of-taking-your-business-into-the-cloud

Cancila, M. (2015). *How to Budget, Track, and Reduce Public Cloud Spending.* Gartner.

Defense Acquisition Regulations System. (2015, August 26). *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)*. Retrieved from FederalRegister.gov: https://federalregister.gov/a/2015-20870

Department of Defense Inspector General. (2014, December 4). *DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process.* Retrieved from DODIG.mil: http://www.dodig.mil/pubs/documents/DODIG-2015-045.pdf

DISA. (2014, May 5). *Enabling the JIE: Shaping the Enterprise for the Conflicts of Tomorrow*. Retrieved from DISA.mil: http://www.disa.mil/About/Our-Work/~/media/Files/DISA/About/JIE101_000.pdf

DISA. (2015, August 6). *Best Practices Guide for Department of Defense Cloud Mission Owners.* Retrieved from DISA.mil: http://iasecontent.disa.mil/stigs/pdf/unclass-best_practices_guide_for_dod_cloud_mission_owners_FINAL.pdf

DISA. (2015, January 12). *Department of Defense Cloud Computing Security Requirements Guide V1, R1*. Retrieved from DISA.mil: http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf

DISA. (2015, September 30). *DoD Cloud Services Catalog*. Retrieved from DISA.mil: https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx

DISA. (n.d.). *milCloud Frequently Asked Questions*. Retrieved from milCloud.mil: https://www.milcloud.mil/support/milCloudFAQs

DOD CIO. (2012, July). *Cloud Computing Strategy.* Retrieved from Defense.gov: http://www.defense.gov/news/DoDCloudComputingStrategy.pdf

GAO. (2012). *Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenace Investments.* Washington: U.S. Government Accountability Office.

Halvorsen, T. (2014, December 15). *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services.* Retrieved from Department of Navy CIO: http://www.doncio.navy.mil/uploads/0105ELX32624.pdf

He, S., & L. Guo, Y. G. (2011). Real Time Elastic Cloud Management for Limited Resources. *Proceedings of 2011 IEEE 4th International Conference on Cloud Computing (Cloud2011)* (pp. 622-629). IEEE.

Hunter, L. (2015, June 17). *DoD's Move to the Cloud: Box it Up or Build New?* Retrieved from MeriTalk: http://meritalk.com/boxorbuild

John Polimeni, K. M. (2007). *The Jevons Paradox and the Myth of Resource Efficiency Improvements.* Earthscan.

Konkel, F. (2014, January 7). *DOD's Cautious Path to the Cloud*. Retrieved from Federal Computer Weekly: http://fcw.com/articles/2014/01/07/dod-cloud-standards.aspx

Mahoney, S. (2014, February 19). *The economics of using cloud accounting systems*. Retrieved from SmartCEO: http://www.smartceo.com/brittenford-economics-using-cloud-accounting-systems/

Martin, J. (2014, May 14). *milCloud.* Retrieved from AFCEA.org: http://www.afcea.org/events/jie/14/documents/MILCLOUD_MARTIN--FINAL.pdf

Masanet, E., Shehabi, A., Ramakrishnan, L., Liang, J., Ma, X., Walker, B., . . . Mantha, P. (2013). *The Energy Efficiency Potential of Cloud-Based Software: A U.S. Case Study.* Berkeley: Lawrence Berkeley National Laboratory.

Mohamed, A. (2009, March). *A history of Cloud Computing*. Retrieved from ComputerWeekly.com: http://www.computerweekly.com/feature/A-history-of-cloud-computing

Moore, G. A. (2014). *Crossing the Chasm, 3rd Edition.* Harper Collins.

NICCS. (n.d.). *A Glossary of Common Cybersecurity Terminology*. Retrieved from National Initiative for Cybersecurity Careers and Studies: http://niccs.us-cert.gov/glossary#incident

NIST. (2011). *SP 800-145: The NIST Definition of Cloud Computing.*

Pellerin, C. (2015, February 26). *DoD CIO Details Information Technology Priorities*. Retrieved from DoD News, Defense Media Activity: http://www.defense.gov/News-Article-View/Article/604182

Pomerleau, M. (2015, July 23). *Air Force, DLA move to Office 365*. Retrieved from GCN.com: http://gcn.com/articles/2015/07/23/af-dla-cloud.aspx

Sauro, J. (2011, November 30). *10 Essential Usability Metrics*. Retrieved from MeasuringU.com: http://www.measuringu.com/blog/essential-metrics.php

Sinnema, R. (. (n.d.). *On Demand Self-Service*. Retrieved from Secure Software Development: http://securesoftwaredev.com/cloud-computing/on-demand-self-service/

Sinnema, R. (. (n.d.). *Rapid Elasticity*. Retrieved from Secure Software Development: http://securesoftwaredev.com/cloud-computing/rapid-elasticity/

Skali Group. (n.d.). *Public Cloud vs Private Cloud*. Retrieved from Skali.net: http://skali.net/public-cloud-vs-private-cloud

Stanton, B., Theofanos, M., & Joshi, K. P. (2015). Framework for Cloud Usability. In T. Tryfonas, & I. Askoxylakis (Ed.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 664-671). Los Angeles, CA: Springer.

Symantec Security Response. (2015, May 13). *VENOM vulnerability could expose virtual machines on unpatched host systems*. Retrieved from Symantec Connect: http://www.symantec.com/connect/blogs/venom-vulnerability-could-expose-virtual-machines-unpatched-host-systems

Takai, T. (2012, June 26). *Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker.* Retrieved from Defense.gov: http://www.defense.gov/news/DISADesignation.pdf

TechTarget. (n.d.). *The history of cloud computing and what's coming next: A CIO guide*. Retrieved from TechTarget.com: http://searchcio.techtarget.com/essentialguide/The-history-of-cloud-computing-and-whats-coming-next-A-CIO-guide

Telford, R. (2012, September). *Relocated or Born There: Different Routes to the Cloud*. Retrieved from Wired.com: http://www.wired.com/insights/2012/09/relocated-or-born-there/

The Open Group. (2013). *Cloud Computing for Business : What is Cloud?* Retrieved from OpenGroup.org: http://www.opengroup.org/cloud/cloud/cloud_for_business/what.htm

Thoughts on Cloud. (2015, April 5). *Cloud through the ages: 1950s to present day*. Retrieved from ThoughtsOnCloud.com: http://www.thoughtsoncloud.com/2015/04/a-brief-history-of-cloud-1950-to-present-day/

USD(AT&L). (2015, February 5). *DFARS Class Deviation 2015-O0011, Contracting for Cloud Services.* Retrieved from Defense Procurement and Acquisition Policy: http://www.acq.osd.mil/dpap/policy/policyvault/USA001321-15-DPAP.pdf

Wexler, J. (2015, July 1). *Moving Legacy Applications to the Cloud? Make Sure You Do It Right*. Retrieved from CIO.com: http://www.cio.com/article/2943262/cloud-apps/moving-legacy-applications-to-the-cloud-make-sure-you-do-it-right.html

What is XaaS. (2010, August). Retrieved July 17, 2015, from http://searchcloudcomputing.techtarget.com/definition/XaaS-anything-as-a-service

Acronyms and Abbreviations

ARPANET	Advanced Research Projects Agency Network
ATO	Authority To Operate
AWS	Amazon Web Services
BCA	Business Case Analysis
CAP	Cloud Access Point
CAPEX	capital expenditure
CIO	Chief Information Officer
CND	Computer Network Defense
CNSSI	Committee on National Security Systems Instruction
COTS	commercial-off-the-shelf
CPU	central processing unit
CRM	Customer Relationship Management
CSO	cloud service offerings
CSP	cloud service provider
CUI	Controlled Unclassified Information
DECC	Defense Enterprise Computing Centers
DEE	DoD Enterprise Email
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIB	defense industrial base
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODIN	DoD Information Network
DRaaS	Disaster Recovery as a Service
EC2	Elastic Compute Cloud

ECSB	Enterprise Cloud Service Broker
FedRAMP	Federal Risk and Authorization Management Program
FIT	Failures In Time
FOUO	For Official Use Only
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HCI	Human-Computer Interaction
HSM	hardware security modules
IaaS	Infrastructure as a Service
IC	Intelligence Community
IDA	Institute for Defense Analyses
IT	information technology
ITAR	International Traffic in Arms Regulations
JAB	Joint Authorization Board
JIE	Joint Information Environment
MaaS	Monitoring as a Service
MTBF	mean time between failures
MTTF	mean time to fail
MTTR	mean time to repair
NIST	National Institute for Standards and Technology
OPEX	operational expenditure
PA	Provisional Authorization
PaaS	Platform as a Service
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RAID	redundant array of inexpensive disks
S3	Simple Storage Service

SaaS	Software as a Service
SDN	software-defined networks
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SRG	Security Requirements Guide
TCO	Total Cost of Ownership
TTP	tactics, techniques, and procedures
US-CERT	United States Computer Emergency Response Team
VDC	Virtual Data Center
VLAN	virtual local area networks
XaaS	Anything as a Service

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-11-15	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Use of Commercial Cloud Computing Capabilities and Services	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Laura Odell, Ryan R. Wagner, Tristan J. Weir	BC-5-3975
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	P-5287 H 15-000865

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
David Cotton Deputy CIO for Information Environment, DoD CIO Pentagon, rm. 3E1041	DoD CIO
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

This papers addresses requests made by both the U.S. House Armed Services Committee and the U.S. Senate Armed Services Committee for independent assessments of the Department of Defense (DoD) approach to using commercial cloud computing. As of 2015, the Department of Defense (DoD) is taking action to offer a wider selection of commercially owned and operated cloud services to DoD mission owners. DoD has instituted a process to evaluate and issue Provisional Authorizations for cloud service offerings, based on the security controls that the provider implements and the sensitivity level of the data that it intends to host. The timing of DoD's move towards the commercial cloud is reasonable given the risk and assurance requirements of many of its missions. However, the Department could offer better guidance about the risks of cloud computing and what mission owners should consider as they mitigate or avoid those risks. We also recommend that DoD consider allowing its Defense Industrial Base partners to participate in high-sensitivity community cloud infrastructure, thereby increasing the efficiency and utility of those systems.

15. SUBJECT TERMS

Cloud computing, metrics, commercial cloud service provider, milCloud, Joint Information Environment, cybersecurity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David Cotton
Unclassified	Unclassified	Unclassified	Unlimited	62	19b. TELEPHONE NUMBER (Include Area Code) 703-695-0871